VA PRIVACY SERVICE

OPM CYBERSECURITY PRIVACY INCIDENT TIP SHEET

The Office of Personnel Management (OPM) provided the information in this fact sheet. For more information, visit https://www.opm.gov/cybersecurity/.

WHAT HAPPENED?

OPM recently discovered **two separate but related cybersecurity incidents** that have impacted the data of Federal government employees, contractors, and others:

1. In April 2015, OPM discovered that the **personnel data of 4.2 million current and former Federal government employees had been stolen.** This means information such as full name, birth date, home address and Social Security Numbers were affected. This number has not changed since it was announced by OPM in early June and **you should have already received a notification if you were impacted.**
2. While investigating this incident, in early June 2015, OPM discovered that additional information had been compromised: including **background investigation records of current, former, and prospective Federal employees and contractors.** OPM and the interagency incident response team have concluded with high confidence that sensitive information, including the Social Security Numbers (SSNs) of 21.5 million individuals, was stolen from the background investigation databases. This includes 19.7 million individuals that applied for a background investigation, and 1.8 million non-applicants, primarily spouses or co-habitants of applicants. Some records also include findings from interviews conducted by background investigators and approximately 1.1 million include fingerprints. Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen. **Notifications for this incident started on September 30, 2015. We estimate notifications will continue for approximately 12 weeks.**

While background investigation records do contain some information regarding mental health and financial history provided by applicants and people contacted during the background investigation, there is no evidence that health, financial, payroll and retirement records of Federal personnel or those who have applied for a Federal job were impacted by this incident (for example, annuity rolls, retirement records, USA JOBS, Employee Express).

OPM and an interagency team from the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) have been investigating these incidents, and are working to put in place changes that will prevent similar thefts in the future. Based on the analysis and forensics to date, the interagency incident response team assesses that the adversary is no longer active on OPM's network.

HOW YOU MAY BE AFFECTED

If your background investigation was conducted any time after the year 2000 (which occurs through the submission of forms SF-86, SF-85, or SF-85P for either a new investigation or a reinvestigation), it is likely that you are affected by the incident involving background investigations. If you completed a background investigation prior to 2000, you may also have been affected, but it is less likely.

VA PRIVACY SERVICE

OPM CYBERSECURITY PRIVACY INCIDENT TIP SHEET

The list below indicates whose information may have been compromised during these incidents. Please visit https://www.opm.gov/cybersecurity/ for detailed information about each category.

- Current and former Federal government employees and contractors
- Job Candidates for Federal employment who were required to complete a background investigation
- Spouses and co-habitants of current and former Federal employees, contractors, and job candidates
- Immediate family, close contacts, and references of current and former Federal employees, contractors, and job candidates

WHAT YOU CAN DO

At this time, there is no information to suggest misuse of the information that was stolen from OPM's systems. We are continuing to investigate and monitor the situation. We have started notifying individuals impacted by the background investigation incident. Those impacted will automatically be eligible for some services and will need to take action to enroll in others.

Visit https://www.opm.gov/cybersecurity/, click on “Cybersecurity Incidents” and select “What You Can Do” in the left navigation panel, to find tips on:

- Spotting the warning signs of identity theft
- Identifying phishing scams
- Updating your passwords
- Learning more about computer security
- Taking next steps if you think your identity has been stolen
- Protecting yourself from exploitation
- Practicing safe online behavior every day

WHAT OPM IS DOING TO HELP

- Sent notifications to those affected by the breach involving personal data.
- Continuing to strengthen cyber defenses at OPM and throughout the Federal government.

VA Privacy Service is a component of the Office of Privacy and Records Management (OPRM), and its mission is to preserve and protect the personally identifiable information of Veterans, their beneficiaries, and VA employees by promoting a culture of privacy awareness and maintaining the trust of those that they serve.